

ON FINITE p -GROUPS WITH ABELIAN AUTOMORPHISM GROUP

VIVEK K. JAIN, PRADEEP K. RAI, AND MANOJ K. YADAV

ABSTRACT. We construct, for the first time, various types of specific non-special finite p -groups having abelian automorphism group. More specifically, we construct groups G with abelian automorphism group such that $\gamma_2(G) < Z(G) < \Phi(G)$, where $\gamma_2(G)$, $Z(G)$ and $\Phi(G)$ denote the commutator subgroup, the center and the Frattini subgroup of G respectively. For a finite p -group G with elementary abelian automorphism group, we show that at least one of the following two conditions holds true: (i) $Z(G) = \Phi(G)$ is elementary abelian; (ii) $\gamma_2(G) = \Phi(G)$ is elementary abelian, where p is an odd prime. We construct examples to show the existence of groups G with elementary abelian automorphism group for which exactly one of the above two conditions holds true.

1. INTRODUCTION

Let G be a finite group. An automorphism α of G is called *central* if $x^{-1}\alpha(x) \in Z(G)$ for all $x \in G$, where $Z(G)$ denotes the center of G . The set of all central automorphisms of G is a normal subgroup of $\text{Aut}(G)$, the group of all automorphisms of G . We denote this group by $\text{Autcent}(G)$. Notice that $\text{Autcent}(G) = C_{\text{Aut}(G)}(\text{Inn}(G))$, the centralizer of $\text{Inn}(G)$ in $\text{Aut}(G)$, and $\text{Autcent}(G) = \text{Aut}(G)$ if $\text{Aut}(G)$ is abelian. We denote the commutator and Frattini subgroup of G with $\gamma_2(G)$ and $\Phi(G)$, respectively. Let $G^{p^i} = \langle x^{p^i} \mid x \in G \rangle$ and $G_{p^i} = \langle x \in G \mid x^{p^i} = 1 \rangle$, where $i \geq 1$ is an integer. For finite abelian groups H and K , $\text{Hom}(H, K)$ denotes the group of all homomorphisms from H to K . If H is a subgroup (proper subgroup) of G , then we write $H \leq G$ ($H < G$). A group G is said to be *purely non-abelian* if it does not have a non-trivial abelian direct factor. Throughout the paper, any unexplained p always denotes an odd prime.

In this paper we construct, for the first time, various types of non-special finite p -groups G such that $\text{Aut}(G)$ is abelian. The story began in 1908 with the following question of H. Hilton [10]: *Whether a non-abelian group can have an abelian group of isomorphisms (automorphisms)*. In 1913, G. A. Miller [17] constructed a non-abelian group G of order 64 such that $\text{Aut}(G)$ is an elementary abelian group of order 128. More examples of such 2-groups were constructed in [4, 14, 20]. For an odd prime p , the first example of a finite p -group G such that $\text{Aut}(G)$ is abelian was constructed by H. Heineken and H. Liebeck [8] in 1974. In 1975, D. Jonah and M. Konvisser [15] constructed 4-generated groups of order p^8 such that $\text{Aut}(G)$ is an elementary abelian group of order p^{16} , where p is any prime. In 1975, by generalizing the constructions of Jonah and Konvisser, B. Earnley [5, Section 4.2] constructed n -generated special p -groups G such that $\text{Aut}(G)$ is abelian, where $n \geq 4$ is an integer and p is any prime number. Among other things, Earnley also proved that there is no p -group G of order p^5 or less such that $\text{Aut}(G)$ is abelian. On the way to constructing finite p -groups of class 2 such that all normal subgroups of G are characteristic, in 1979 H. Heineken [9] produced groups G such that $\text{Aut}(G)$ is abelian. In 1994, M. Morigi [18] proved that there exists

2010 *Mathematics Subject Classification*. Primary 20D45; Secondary 20D15.

Key words and phrases. finite p -group, central automorphism, abelian automorphism group.

no group of order p^6 whose group of automorphisms is abelian and constructed groups G of order p^{n^2+3n+3} such that $\text{Aut}(G)$ is abelian, where n is a positive integer. In particular, for $n = 1$, it provides a group of order p^7 having an abelian automorphism group.

There have also been attempts to get structural information of finite groups having abelian automorphism group. In 1927, C. Hopkins [11], among other things, proved that a finite p -group G such that $\text{Aut}(G)$ is abelian, can not have a non-trivial abelian direct factor. In 1995, M. Morigi [19] proved that the minimal number of generators for a p -group with abelian automorphism group is 4. In 1995, P. Hegarty [7] proved that if G is a non-abelian p -group such that $\text{Aut}(G)$ is abelian, then $|\text{Aut}(G)| \geq p^{12}$, and the minimum is obtained by the group of order p^7 constructed by M. Morigi. Moreover, in 1998, G. Ban and S. Yu [2] obtained independently the same result and proved that if G is a group of order p^7 such that $\text{Aut}(G)$ is abelian, then $|\text{Aut}(G)| = p^{12}$.

We remark here that all the examples (for an odd prime p) mentioned above are special p -groups. In 2008, A. Mahalanobis [16] published the following conjecture: *For an odd prime p , any finite p -group having abelian automorphism group is special.* The first and third authors [13] provided counter examples to this conjecture by constructing a class of non-special finite p -groups G such that $\text{Aut}(G)$ is abelian. These counter examples, constructed in [13], enjoy the following properties: (i) $|G| = p^{n+5}$, where p is an odd prime and n is an integer ≥ 3 ; (ii) $\gamma_2(G)$ is a proper subgroup of $Z(G) = \Phi(G)$; (iii) exponents of $Z(G)$ and $G/\gamma_2(G)$ are same and it is equal to p^{n-1} ; (iv) $\text{Aut}(G)$ is abelian of exponent p^{n-1} .

Having all this information in hands, one might expect that some weaker form of the conjecture of Mahalanobis still holds true. Two obvious weaker forms of the conjecture are: (WC1) For a finite p -group G with $\text{Aut}(G)$ abelian, $Z(G) = \Phi(G)$ always holds true; (WC2) For a finite p -group G with $\text{Aut}(G)$ abelian and $Z(G) \neq \Phi(G)$, $\gamma_2(G) = Z(G)$ always holds true. So, on the way to exploring some general structure on the class of such groups G , it is natural to ask the following question:

Question. Does there exist a finite p -group G such that $\gamma_2(G) \leq Z(G) < \Phi(G)$ and $\text{Aut}(G)$ is abelian?

Disproving (WC1) and (WC2), we provide affirmative answer to this question, in the following theorem, which we prove in Section 3:

Theorem A. *For every positive integer $n \geq 4$ and every odd prime p , there exists a group G of order p^{n+10} and exponent p^n such that*

- (1) *for $n = 4$, $\gamma_2(G) = Z(G) < \Phi(G)$ and $\text{Aut}(G)$ is abelian;*
- (2) *for $n \geq 5$, $\gamma_2(G) < Z(G) < \Phi(G)$ and $\text{Aut}(G)$ is abelian.*

Moreover, the order of $\text{Aut}(G)$ is p^{n+20} .

One more weaker form of the above said conjecture is: (WC3) If $\text{Aut}(G)$ is an elementary abelian p -group, then G is special. As remarked above, all p -groups G (except the ones in [13]) available in the literature and having abelian automorphism group are special p -groups. Thus it follows that $\text{Aut}(G)$, for all such groups G , is elementary abelian. Y. Berkovich and Z. Janko [3, Problem 722] published the following long standing problem: *(Old problem) Study the p -groups G with elementary abelian $\text{Aut}(G)$.*

Let G be an arbitrary finite p -group such that $\text{Aut}(G)$ is elementary abelian. Then it follows from Theorem 4.1 (proved in Section 4 below) that one of the following two conditions necessarily holds true: (C1) $Z(G) = \Phi(G)$ is elementary abelian; (C2) $\gamma_2(G) = \Phi(G)$ is elementary abelian. *So one might expect that for such groups G both of the conditions (C1) and (C2) hold true, i.e., $WC(3)$ holds true, or, a little less ambitiously, (C1) always holds true or (C2) always holds true.* In the following two theorems, which we prove in Section 4, we show that none of the statements in the preceding sentence holds true.

Theorem B. *There exists a group G of order p^9 such that $\text{Aut}(G)$ is elementary abelian of order p^{20} , $\Phi(G) < Z(G)$ and $\gamma_2(G) = \Phi(G)$ is elementary abelian.*

Theorem C. *There exists a group G of order p^8 such that $\text{Aut}(G)$ is elementary abelian of order p^{16} , $\gamma_2(G) < \Phi(G)$ and $Z(G) = \Phi(G)$ is elementary abelian.*

Now we review non-special 2-groups having abelian automorphism group. In contrast to p -groups for odd primes, there do exist finite 2-groups G with $\text{Aut}(G)$ abelian and G satisfies either of the following two properties: (P1) G is 3-generated; (P2) G has a non-trivial abelian direct factor. The first 2-group having abelian automorphism group was constructed by G. A. Miller [17] in 1913. This is a 3-generated group and, as mentioned above, it has order 64 with elementary abelian automorphism group of order 128. B. Earnley [5] showed that there are two more groups of order 64 having elementary abelian automorphism group. These groups are also 3-generated. Further B. Earnley [5, Theorem 2.3] gave a complete description of 2-groups satisfying (P2) and having abelian automorphism group and established the existence of such groups.

Let G be a purely non-abelian finite 2-group such that $\text{Aut}(G)$ is elementary abelian. Thus $\text{Aut}(G) = \text{Autcent}(G)$. Then G satisfies one of the three conditions of Theorem 2.2. We here record that there exist groups G which satisfy exactly one condition of this theorem. It is easy to show that the 2-group G_2 constructed in (4.1) satisfies only the first condition of Theorem 2.2 and the 2-group G_3 constructed in (4.7) satisfies only the second condition of Theorem 2.2. That $\text{Aut}(G_2)$ and $\text{Aut}(G_3)$ are elementary abelian, can be checked using GAP [6]. The examples of 2-groups G satisfying only the third condition of Theorem 2.2 with $\text{Aut}(G)$ elementary abelian were constructed by A. Miller [17] and M. J. Curran [4].

The examples constructed in Theorems A, B and C indicate that it is difficult to put an obvious structure on the class of groups G such that $\text{Aut}(G)$ is abelian or even elementary abelian. We hope that this paper will be helpful in giving a direction to the research area under consideration. We remark that many non-isomorphic groups, satisfying the conditions of the above theorems, can be obtained by making suitable changes in the presentations given in (3.1), (4.1) and (4.7) below. We conclude this section with a further remark that the kind of examples constructed here may be useful in cryptography (see [16] for more details).

2. SOME PREREQUISITES AND BASIC RESULTS

We start with the following two theorems of M. H. Jafari [12].

Theorem 2.1 (Theorem 3.4). *Let G be a finite purely nonabelian p -group, p odd, then $\text{Autcent}(G)$ is an elementary abelian p -group if and only if the exponent of $Z(G)$ is p or exponent of $G/\gamma_2(G)$ is p .*

A finite abelian p -group G is said to be *ce-group* if G can be written as a direct product of a cyclic group A of order p^n , $n > 1$ and an elementary abelian p -group B .

Theorem 2.2 (Theorem 3.5). *Let G be a purely nonabelian 2-group. Then $\text{Autcent}(G)$ is elementary abelian if and only if one of the following conditions holds:*

- (1) *the exponent of $G/\gamma_2(G)$ is 2;*
- (2) *the exponent of $Z(G)$ is 2;*
- (3) *the greatest common divisor of the exponents of $G/\gamma_2(G)$ and $Z(G)$ is 4 and $G/\gamma_2(G)$, $Z(G)$ are ce-groups having the properties that an elementary part of $Z(G)$ is contained in $\gamma_2(G)$ and there exists an element z of order 4 in a cyclic part of $Z(G)$ with $z\gamma_2(G)$ lying in a cyclic part of $G/\gamma_2(G)$ such that twice of the order of $z\gamma_2(G)$ is equal to the exponent of $G/\gamma_2(G)$.*

The next result is by B. Earnley [5, Corollary 3.3].

Theorem 2.3. *Let G be a non-abelian finite p -group of exponent p , where p is an odd prime. Then $\text{Aut}(G)$ is non-abelian.*

The following two results are well known.

Lemma 2.4. *Let A , B and C be finite abelian groups. Then $\text{Hom}(A \times B, C) \cong \text{Hom}(A, C) \times \text{Hom}(B, C)$ and $\text{Hom}(A, B \times C) \cong \text{Hom}(A, B) \times \text{Hom}(A, C)$.*

Lemma 2.5. *Let C_r and C_s be two cyclic groups of order r and s respectively. Then $\text{Hom}(C_r, C_s) \cong C_d$, where d is the greatest common divisor of r and s .*

The following result follows from [1, Theorem 1].

Proposition 2.6. *Let G be a purely non-abelian finite p -group. Then $|\text{Autcent}(G)| = |\text{Hom}(G/\gamma_2(G), Z(G))|$.*

Let A be an abelian p -group and $a \in A$. For a positive integer n , p^n is said to be the *height* of a in A , denoted by $\text{ht}(a)$, if $a \in A^{p^n}$ but $a \notin A^{p^{n+1}}$. Let H be a p -group of class 2. We denote the exponents of $Z(H)$, $\gamma_2(H)$, $H/\gamma_2(H)$ by p^a , p^b , p^c respectively and $d = \min(a, c)$. We define $R := \{z \in Z(H) \mid |z| \leq p^d\}$ and $K := \{x \in H \mid \text{ht}(x\gamma_2(H)) \geq p^b\}$. Notice that $K = H^{p^b}\gamma_2(H)$. Now we state the following important result of J. E. Adney and T. Yen [1, Theorem 4] (in our notations).

Theorem 2.7. *Let H be a purely non-abelian p -group of class 2, p odd, and let $H/\gamma_2(H) = \Pi_{i=1}^n \langle x_i\gamma_2(H) \rangle$. Then $\text{Autcent}(H)$ is abelian if and only if*

- (i) $R = K$, and
- (ii) *either $d = b$ or $d > b$ and $R/\gamma_2(H) = \langle x_1^{p^b}\gamma_2(H) \rangle$.*

Let G be a finite p -group of nilpotency class 2 generated by x_1, x_2, \dots, x_d , where d is a positive integer. Let $e_{x_i} = x_1^{a_{i1}} x_2^{a_{i2}} \cdots x_d^{a_{id}} = \prod_{j=1}^d x_j^{a_{ij}}$, where $x_i \in G$ and a_{ij} are non-negative integers for $1 \leq i, j \leq d$. Since the nilpotency class of G is 2, we have

$$(2.1) \quad [x_k, e_{x_i}] = [x_k, \prod_{j=1}^d x_j^{a_{ij}}] = \prod_{j=1}^d [x_k, x_j^{a_{ij}}] = \prod_{j=1}^d [x_k, x_j]^{a_{ij}}$$

and

$$(2.2) \quad \begin{aligned} [e_{x_k}, e_{x_i}] &= [\prod_{l=1}^d x_l^{a_{kl}}, \prod_{j=1}^d x_j^{a_{ij}}] = \prod_{j=1}^d \prod_{l=1}^d [x_l^{a_{kl}}, x_j^{a_{ij}}] \\ &= \prod_{j=1}^d \prod_{l=1}^d [x_l, x_j]^{a_{kl} a_{ij}}. \end{aligned}$$

Equations (2.1) and (2.2) will be used for our calculations without any further reference.

3. GROUPS G WITH $\text{Aut}(G)$ ABELIAN

In this section we construct a class of finite p -groups such that $\gamma_2(G) \leq Z(G) < \Phi(G)$ and $\text{Aut}(G)$ is abelian. Let $n \geq 4$ be a positive integer and p be an odd prime. Consider the following group:

$$(3.1) \quad G = \left\langle x_1, x_2, x_3, x_4 \mid x_1^{p^n} = x_2^{p^4} = x_3^{p^4} = x_4^{p^2} = 1, [x_1, x_2] = x_2^{p^2}, \right. \\ [x_1, x_3] = x_2^{p^2}, [x_1, x_4] = x_3^{p^2}, [x_2, x_3] = x_1^{p^{n-2}}, [x_2, x_4] = x_3^{p^2}, \\ \left. [x_3, x_4] = x_2^{p^2} \right\rangle.$$

Throughout this section, G always denotes the group given in (3.1). It is easy to see that G enjoys the properties given in the following lemma.

Lemma 3.1. *The group G is a regular p -group of nilpotency class 2 having order p^{n+10} and exponent p^n . For $n = 4$, $\gamma_2(G) = Z(G) < \Phi(G)$ and for $n \geq 5$, $\gamma_2(G) < Z(G) < \Phi(G)$.*

Let $e_{x_i} = x_1^{a_{i1}} x_2^{a_{i2}} x_3^{a_{i3}} x_4^{a_{i4}} = \prod_{j=1}^4 x_j^{a_{ij}}$, where $x_i \in G$ and a_{ij} are non-negative integers for $1 \leq i, j \leq 4$. Let α be an automorphism of G . Since the nilpotency class of G is 2 and $\gamma_2(G)$ is generated by $x_1^{p^{n-2}}, x_2^{p^2}, x_3^{p^2}$, we can write $\alpha(x_i) = x_i e_{x_i} = x_i \prod_{j=1}^4 x_j^{a_{ij}}$ for some non-negative integers a_{ij} for $1 \leq i, j \leq 4$.

Proposition 3.2. *Let G be the group defined in (3.1) and α be an automorphism of G such that $\alpha(x_i) = x_i e_{x_i} = x_i \prod_{j=1}^4 x_j^{a_{ij}}$, where a_{ij} are some non-negative integers for $1 \leq i, j \leq 4$. Then the*

following equations hold:

$$\begin{aligned}
(3.2) \quad & a_{31} \equiv 0 \pmod{p^{n-2}}, \\
(3.3) \quad & -a_{32} + a_{13} + a_{13}a_{44} \equiv 0 \pmod{p^2}, \\
(3.4) \quad & -a_{33} + a_{44} + a_{11} + a_{11}a_{44} + a_{12} + a_{12}a_{44} \equiv 0 \pmod{p^2}, \\
(3.5) \quad & a_{21} \equiv 0 \pmod{p^{n-2}}, \\
(3.6) \quad & a_{44} - a_{22} + a_{33} + a_{33}a_{44} \equiv 0 \pmod{p^2}, \\
(3.7) \quad & a_{32} - a_{23} + a_{32}a_{44} \equiv 0 \pmod{p^2}, \\
(3.8) \quad & -a_{13} + a_{12}a_{23} - a_{13}a_{22} \equiv 0 \pmod{p^2}, \\
(3.9) \quad & a_{23} + a_{11} + a_{11}a_{22} + a_{11}a_{23} + a_{13}a_{24} - a_{14}a_{23} \equiv 0 \pmod{p^2}, \\
(3.10) \quad & -a_{23} + a_{24} + a_{11}a_{24} - a_{14} + a_{12}a_{24} - a_{14}a_{22} \equiv 0 \pmod{p^2}, \\
(3.11) \quad & a_{12} + a_{12}a_{33} - a_{13}a_{32} \equiv 0 \pmod{p^2}, \\
(3.12) \quad & a_{32} + a_{33} + a_{11} - a_{22} - a_{14} + a_{11}a_{32} + a_{11}a_{33} + a_{13}a_{34} - a_{14}a_{33} \\
& \equiv 0 \pmod{p^2}, \\
(3.13) \quad & a_{34} + a_{11}a_{34} + a_{12}a_{34} - a_{14}a_{32} - a_{23} \equiv 0 \pmod{p^2}, \\
(3.14) \quad & a_{23} - a_{32} + a_{23}a_{44} \equiv 0 \pmod{p^2}, \\
(3.15) \quad & -a_{33} + a_{44} + a_{22} + a_{22}a_{44} \equiv 0 \pmod{p^2}, \\
(3.16) \quad & -a_{11} + a_{33} + a_{22} + a_{22}a_{33} - a_{23}a_{32} \equiv 0 \pmod{p^2}.
\end{aligned}$$

Proof. Let α be the automorphism of G such that $\alpha(x_i) = x_i e_{x_i}$, $1 \leq i \leq 4$ as defined above. Since $G_{p^2} = \langle x_1^{p^{n-2}}, x_2^{p^2}, x_3^{p^2}, x_4 \rangle$ is a characteristic subgroup of G , $\alpha(x_4) \in G_{p^2}$. Thus we get the following set of equations:

$$\begin{aligned}
(3.17) \quad & a_{41} \equiv 0 \pmod{p^{n-2}}, \\
(3.18) \quad & a_{4i} \equiv 0 \pmod{p^2}, \text{ for } i = 2, 3.
\end{aligned}$$

We prove equations (3.2) - (3.4) by comparing the powers of x_i 's in $\alpha([x_1, x_4]) = \alpha(x_3^{p^2})$.

$$\begin{aligned}
\alpha([x_1, x_4]) &= [\alpha(x_1), \alpha(x_4)] = [x_1 e_{x_1}, x_4 e_{x_4}] \\
&= [x_1, x_4][x_1, e_{x_4}][e_{x_1}, x_4][e_{x_1}, e_{x_4}] \\
&= [x_1, x_4] \prod_{j=1}^4 [x_1, x_j]^{a_{4j}} \prod_{j=1}^4 [x_4, x_j]^{-a_{1j}} \prod_{j=1}^4 \prod_{l=1}^4 [x_l, x_j]^{a_{1l}a_{4j}} \\
&= [x_1, x_2]^{a_{42}+a_{11}a_{42}-a_{12}a_{41}} [x_1, x_3]^{a_{43}+a_{11}a_{43}-a_{13}a_{41}} \\
&\quad [x_1, x_4]^{1+a_{44}+a_{11}+a_{11}a_{44}-a_{14}a_{41}} [x_2, x_3]^{a_{12}a_{43}-a_{13}a_{42}} \\
&\quad [x_2, x_4]^{a_{12}+a_{12}a_{44}-a_{14}a_{42}} [x_3, x_4]^{a_{13}+a_{13}a_{44}-a_{14}a_{43}} \\
&= x_1^{p^{n-2}(a_{12}a_{43}-a_{13}a_{42})} \\
&\quad x_2^{p^2(a_{42}+a_{43}+a_{13}+a_{11}a_{42}-a_{12}a_{41}+a_{11}a_{43}-a_{13}a_{41}+a_{13}a_{44}-a_{14}a_{43})} \\
&\quad x_3^{p^2(1+a_{44}+a_{11}+a_{12}+a_{11}a_{44}-a_{14}a_{41}+a_{12}a_{44}-a_{14}a_{42})}.
\end{aligned}$$

On the other hand

$$\alpha([x_1, x_4]) = \alpha(x_3^{p^2}) = x_3^{p^2} x_1^{p^2 a_{31}} x_2^{p^2 a_{32}} x_3^{p^2 a_{33}} x_4^{p^2 a_{24}} = x_1^{p^2 a_{31}} x_2^{p^2 a_{32}} x_3^{p^2(1+a_{33})}.$$

Comparing the powers of x_1 and using (3.18), we get $a_{31} \equiv 0 \pmod{p^{n-2}}$. Comparing the powers of x_2 and x_3 , and using (3.17) - (3.18), we get

$$\begin{aligned} -a_{32} + a_{13} + a_{13}a_{44} &\equiv 0 \pmod{p^2}, \\ -a_{33} + a_{44} + a_{11} + a_{11}a_{44} + a_{12} + a_{12}a_{44} &\equiv 0 \pmod{p^2}. \end{aligned}$$

Hence equations (3.2) - (3.4) hold.

Equations (3.5) - (3.7) are obtained by comparing the powers of x_1 , x_2 and x_3 in $\alpha([x_3, x_4]) = \alpha(x_2^{p^2})$ and using equations (3.2), (3.17) and (3.18). Equations (3.8) - (3.10) are obtained by comparing the powers of x_1 , x_2 and x_3 in $\alpha([x_1, x_2]) = \alpha(x_2^{p^2})$ and using equation (3.5). Equations (3.11) - (3.13) are obtained by comparing the powers of x_1 , x_2 and x_3 in $\alpha([x_1, x_3]) = \alpha(x_2^{p^2})$ and using equations (3.2) and (3.5). Equations (3.14) - (3.15) are obtained by comparing the powers of x_2 and x_3 in $\alpha([x_2, x_4]) = \alpha(x_3^{p^2})$ and using equations (3.5), (3.17) and (3.18). The last equation (3.16) is obtained by comparing the powers of x_1 in $\alpha([x_2, x_3]) = \alpha(x_1^{p^{n-2}})$.

Theorem 3.3. *Let G be the group defined in (3.1). Then all automorphisms of G are central.*

Proof. We start with the claim that $1 + a_{44} \not\equiv 0 \pmod{p}$. For, let us assume the contrary, i.e., p divides $1 + a_{44}$. Then

$$\alpha(x_4^p) = \alpha(x_4)^p = x_4^{p(1+a_{44})} (x_1^{a_{41}} x_2^{a_{42}} x_3^{a_{43}})^p \in Z(G),$$

since $a_{4j} \equiv 0 \pmod{p^2}$ for $1 \leq j \leq 3$ by equations (3.17) and (3.18). But this is not possible as $x_4^p \notin Z(G)$. This proves our claim. Subtracting (3.14) from (3.3), we get $(1 + a_{44})(a_{13} - a_{23}) \equiv 0 \pmod{p^2}$. Since p does not divide $1 + a_{44}$, we get

$$(3.19) \quad a_{13} \equiv a_{23} \pmod{p^2}.$$

By equations (3.8) and (3.19) we have

$$(3.20) \quad a_{13}(1 - a_{12} + a_{22}) \equiv 0 \pmod{p^2}.$$

Here we have three possibilities, namely (i) $a_{13} \equiv 0 \pmod{p^2}$, (ii) $a_{13} \equiv 0 \pmod{p}$, but $a_{13} \not\equiv 0 \pmod{p^2}$, (iii) $a_{13} \not\equiv 0 \pmod{p}$. We are going to show that cases (ii) and (iii) do not occur and in the case (i) $a_{ij} \equiv 0 \pmod{p^2}$, $1 \leq i, j \leq 4$.

Case (i). Assume that $a_{13} \equiv 0 \pmod{p^2}$. Equations (3.7) and (3.19), together with the fact that p does not divide $1 + a_{44}$, gives $a_{32} \equiv 0 \pmod{p^2}$. We claim that $1 + a_{33} \not\equiv 0 \pmod{p}$. Suppose p divides $1 + a_{33}$. Since $a_{32} \equiv 0 \pmod{p^2}$ and $a_{31} \equiv 0 \pmod{p^{n-2}}$ (equation (3.2)), we get $\alpha(x_3^{p^3}) = x_1^{p^3 a_{31}} x_2^{p^3 a_{32}} x_3^{p^3(1+a_{33})} x_4^{p^3 a_{34}} = 1$, which is not possible. This proves our claim. So by equation (3.11), we get $a_{12} \equiv 0 \pmod{p^2}$.

Subtracting (3.15) from (3.4), we get $(a_{11} - a_{22})(1 + a_{44}) \equiv 0 \pmod{p^2}$. This implies that $a_{11} - a_{22} \equiv 0 \pmod{p^2}$. Since $a_{i3} \equiv 0 \pmod{p^2}$ for $i = 1, 2$, by equation (3.9) we get $a_{11}(1 + a_{11}) \equiv 0 \pmod{p^2}$. Thus p^2 divides a_{11} or $1 + a_{11}$. We claim that p^2 can not divide $1 + a_{11}$. For, suppose the contrary, i. e., $a_{11} \equiv -1 \pmod{p^2}$. Since $n - 2 \geq 2$ and $a_{12} \equiv a_{13} \equiv 0 \pmod{p^2}$, we get

$$\alpha(x_1)^{p^{n-2}} = x_1^{p^{n-2}(1+a_{11})} x_2^{p^{n-2}a_{12}} x_3^{p^{n-2}a_{13}} x_4^{p^{n-2}a_{14}} = 1.$$

This contradiction, to the fact that order of x_1 is p^n , proves our claim. Hence p^2 divides a_{11} . Since $a_{11} - a_{22} \equiv 0 \pmod{p^2}$, by equation (3.15), it follows that $a_{33} \equiv a_{44} \pmod{p^2}$. Putting the values a_{23} , a_{11} and a_{22} in (3.16), we get $a_{33} \equiv 0 \pmod{p^2}$. Thus $a_{44} \equiv 0 \pmod{p^2}$. Putting values of a_{32} ,

a_{33} , a_{11} , a_{22} and a_{13} in (3.12), we get $a_{14} \equiv 0 \pmod{p^2}$. Putting values of a_{12} , a_{14} , a_{11} and a_{23} in (3.13), we get $a_{34} \equiv 0 \pmod{p^2}$. Putting above values in (3.10), we get $a_{24} \equiv 0 \pmod{p^2}$. Hence $a_{ij} \equiv 0 \pmod{p^2}$ for $1 \leq i, j \leq 4$.

Case (ii). Assume that $a_{13} \equiv 0 \pmod{p}$, but $a_{13} \not\equiv 0 \pmod{p^2}$. Equation (3.20) implies that $(1 - a_{12} + a_{22}) \equiv 0 \pmod{p}$. Now consider all the equations (3.5)-(3.16) \pmod{p} . Repeating the arguments of Case (i) after replacing p^2 by p , we get the following facts: (a) $a_{32} \equiv 0 \pmod{p}$ (by (3.7)); (b) $a_{12} \equiv 0 \pmod{p}$ (by (3.11)); (c) $a_{11} - a_{22} \equiv 0 \pmod{p}$ (subtracting (3.15) from (3.4)); (d) $a_{11}(1 + a_{11}) \equiv 0 \pmod{p}$ (by (3.9)). We claim that $a_{11} \equiv 0 \pmod{p}$. For, suppose that $a_{11} + 1 \equiv 0 \pmod{p}$. Since $n - 1 \geq 3$ and $a_{12} \equiv a_{13} \equiv 0 \pmod{p}$, it follows that $\alpha(x_1)^{p^{n-1}} = x_1^{p^{n-1}(1+a_{11})} x_2^{p^{n-1}a_{12}} x_3^{p^{n-1}a_{13}} x_4^{p^{n-1}a_{14}} = 1$, which is a contradiction. This proves that p can not divide $a_{11} + 1$. Hence p divides a_{11} , and therefore by fact (c), we have $a_{22} \equiv 0 \pmod{p}$. This gives a contradiction to the fact that $(1 - a_{12} + a_{22}) \equiv 0 \pmod{p}$. Thus Case (ii) does not occur.

Case (iii). Finally assume that $a_{13} \not\equiv 0 \pmod{p}$. Thus $(1 - a_{12} + a_{22}) \equiv 0 \pmod{p^2}$, i.e., $1 + a_{22} \equiv a_{12} \pmod{p^2}$ (we'll use this information throughout the remaining proof without referring). Notice that $(\alpha(x_2 x_1^{-1}))^{p^2} = x_1^{-p^2(1+a_{11})}$. Since the order of $(\alpha(x_2 x_1^{-1}))^{p^2}$ is p^{n-2} , p does not divide $(1 + a_{11})$. Putting the value of a_{32} from (3.14) into (3.7), we have $a_{23} = a_{23}(1 + a_{44})^2 \pmod{p^2}$. Since $a_{23} \equiv a_{13} \pmod{p^2}$ (equation (3.19)) and $a_{13} \not\equiv 0 \pmod{p}$, it follows that $a_{23} \not\equiv 0 \pmod{p}$. Hence $(1 + a_{44})^2 \equiv 1 \pmod{p^2}$. This gives $a_{44}(a_{44} + 2) \equiv 0 \pmod{p^2}$. Thus we have three cases (iii)(a) $a_{44} \equiv 0 \pmod{p^2}$, (iii)(b) $a_{44} \equiv 0 \pmod{p}$, but $a_{44} \not\equiv 0 \pmod{p^2}$ and (iii)(c) $a_{44} \not\equiv 0 \pmod{p}$. We are going to consider these cases one by one.

Case (iii)(a). Suppose that $a_{44} \equiv 0 \pmod{p^2}$. Using this in (3.14) and (3.15), we get $a_{32} \equiv a_{23} \pmod{p^2}$ and $a_{22} \equiv a_{33} \pmod{p^2}$ respectively. Putting the value of a_{44} in (3.4), we have $a_{12} + a_{11} \equiv a_{33} \pmod{p^2}$. Further, replacing a_{12} by $1 + a_{22}$ and a_{22} by a_{33} , we have $1 + a_{11} \equiv 0 \pmod{p^2}$, which is a contradiction.

Case (iii)(b). Suppose that $a_{44} \equiv 0 \pmod{p}$, but $a_{44} \not\equiv 0 \pmod{p^2}$. Notice that by reading the equations \pmod{p} , arguments of Case (iii)(a) show that $1 + a_{11} \equiv 0 \pmod{p}$, which is again a contradiction.

Case (iii)(c). Suppose that $a_{44} \not\equiv 0 \pmod{p}$. This implies that $a_{44} \equiv -2 \pmod{p^2}$. Putting this value of a_{44} in the difference of (3.6) and (3.4), we get $a_{11} + a_{12} - a_{22} \equiv 0 \pmod{p^2}$. Since $1 + a_{22} \equiv a_{12} \pmod{p^2}$, this equation contradicts the fact that $1 + a_{11} \not\equiv 0 \pmod{p}$.

Thus Case (iii) can not occur. This completes the proof of the theorem. \square

Now we are ready to prove Theorem A stated in the introduction.

Proof of Theorem A. Let G be the group defined in (3.1). By Lemma 3.1, we have $|G| = p^{n+10}$, $\gamma_2(G) = Z(G) < \Phi(G)$ for $n = 4$ and $\gamma_2(G) < Z(G) < \Phi(G)$ for $n \geq 5$. By Theorem 3.3, we have $\text{Aut}(G) = \text{Autcent}(G)$. Thus to complete the proof of the theorem, it is sufficient to prove that $\text{Autcent}(G)$ is an abelian group. Since $Z(G) < \Phi(G)$, G is purely non-abelian. The exponents of $Z(G)$, $\gamma_2(G)$ and $G/\gamma_2(G)$ are p^{n-2} , p^2 and p^{n-2} respectively. Thus we get

$$R = \{z \in Z(G) \mid |z| \leq p^{n-2}\} = Z(G)$$

and

$$K = \{x \in G \mid \text{ht}(x\gamma_2(G)) \geq p^2\} = G^{p^2}\gamma_2(G) = Z(G).$$

This shows that $R = K$. Also $R/\gamma_2(G) = Z(G)/\gamma_2(G) = \langle x_1^{p^2}\gamma_2(G) \rangle$. Thus all the conditions of Theorem 2.7 are now satisfied. Hence $\text{Autcent}(G)$ is abelian. That the order of $\text{Aut}(G)$ is p^{n+20} can be easily proved by using Lemmas 2.4, 2.5, Proposition 2.6 and the structures of $G/\gamma_2(G)$ and $Z(G)$. This completes the proof of the theorem. \square

4. GROUPS G WITH $\text{Aut}(G)$ ELEMENTARY ABELIAN

In this section we construct p -groups with elementary abelian automorphism group. We start with the following result, which provides some structural information of a group G for which $\text{Aut}(G)$ is elementary abelian.

Theorem 4.1. *Let G be a finite p -group such that $\text{Aut}(G)$ is elementary abelian, where p is an odd prime. Then one of the following two conditions holds true:*

- (1) $Z(G) = \Phi(G)$ is elementary abelian;
- (2) $\gamma_2(G) = \Phi(G)$ is elementary abelian.

Moreover, the exponent of G is p^2 .

Proof. Since $\text{Aut}(G)$ is elementary abelian, $G/Z(G)$ is elementary abelian and it follows from a result of Hopkins [11, Section 3] that G is purely non-abelian. It follows from Theorem 2.1 that either $Z(G)$ or $G/\gamma_2(G)$ is of exponent p . If the exponent of $Z(G)$ is p , then $Z(G) \leq \Phi(G)$. Indeed, if $\Phi(G) < Z(G)$, then G has a non-trivial abelian direct factor, which is not possible as G is purely non-abelian. Hence $Z(G) = \Phi(G)$ is elementary abelian. If the exponent of $G/\gamma_2(G)$ is p , then obviously $\gamma_2(G) = \Phi(G)$. Since the exponent of $\gamma_2(G)$ is equal to the exponent of $G/Z(G)$, it follows that $\gamma_2(G) = \Phi(G)$ is elementary abelian. In any case the exponent of $\Phi(G)$ is p . Thus the exponent of G is at most p^2 . That the exponent of G can not be p , follows from Theorem 2.3. Hence the exponent of G is p^2 . This completes the proof of the theorem. \square

Now we proceed to construct p -group G such that $\Phi(G) < Z(G)$, and $\text{Aut}(G)$ and $\gamma_2(G) = \Phi(G)$ are elementary abelian. Let p be any prime, even or odd. Consider the group

$$(4.1) \quad G_1 = \langle x_1, x_2, x_3, x_4, x_5 \mid x_1^{p^2} = x_2^{p^2} = x_3^{p^2} = x_4^{p^2} = x_5^p = 1, [x_1, x_2] = x_1^p, \\ [x_1, x_3] = x_3^p, [x_1, x_4] = 1, [x_1, x_5] = x_1^p, [x_2, x_3] = x_2^p, [x_2, x_4] = 1, \\ [x_2, x_5] = x_4^p, [x_3, x_4] = 1, [x_3, x_5] = x_4^p, [x_4, x_5] = 1 \rangle.$$

It is easy to see the following properties of G_1 .

Lemma 4.2. *The group G_1 is a p -group having order p^9 , $\gamma_2(G_1) = \Phi(G_1) < Z(G_1)$, $\Phi(G_1)$ is elementary abelian and the exponent of $Z(G_1)$ is p^2 , where p is any prime. Moreover, if p is odd, then G_1 is regular.*

As mentioned in the introduction, it can be checked by using GAP that for $p = 2$, $\text{Aut}(G_1)$ is elementary abelian. So we assume that p is odd. For $1 \leq i \leq 5$, let $e_{x_i} = x_1^{a_{i1}} x_2^{a_{i2}} x_3^{a_{i3}} x_4^{a_{i4}} x_5^{a_{i5}}$, where a_{ij} are non-negative integers for $1 \leq i, j \leq 5$. Let α be an arbitrary automorphism of G_1 .

Since the nilpotency class of G_1 is 2 and $\gamma_2(G_1)$ is generated by the set $\{x_i^p \mid 1 \leq i \leq 4\}$, we can write

$$(4.2) \quad \alpha(x_i) = x_i \prod_{j=1}^5 x_j^{a_{ij}}$$

for some non-negative integers a_{ij} for $1 \leq i, j \leq 5$.

Lemma 4.3. *Let α be the automorphism of G_1 defined in (4.2). Then*

$$(4.3) \quad a_{4j} \equiv 0 \pmod{p} \text{ for } j = 1, 2, 3, 5.$$

Proof. Since $x_4 \in Z(G_1)$, it follows that $\alpha(x_4) = x_4^{1+a_{44}} x_1^{a_{41}} x_2^{a_{42}} x_3^{a_{43}} x_5^{a_{45}} \in Z(G_1)$. This is possible only when $a_{4j} \equiv 0 \pmod{p}$ for $j = 1, 2, 3, 5$, which completes the proof of the lemma. \square

We'll make use of the following table in the proof of Theorem B, which is produced in the following way. The equation in the k th row is obtained by applying α on the relation in k th row, then comparing the powers of x_i in the same row, and using preceding equations in the table and equations (4.3). For example, equation in 5th row is obtained by applying α on $[x_1, x_3] = x_3^p$, then comparing the powers of x_2 and using equations in 2nd and 3rd row.

No.	equations	relations	x_i 's
1	$a_{5j} \equiv 0 \pmod{p}, 1 \leq j \leq 4$	$x_5^p = 1$	x_1, x_2, x_3, x_4
2	$a_{12} \equiv 0 \pmod{p}$	$[x_1, x_5] = x_1^p$	x_2
3	$a_{13} \equiv 0 \pmod{p}$	$[x_1, x_5] = x_1^p$	x_3
4	$a_{14} \equiv 0 \pmod{p}$	$[x_1, x_5] = x_1^p$	x_4
5	$a_{32} \equiv 0 \pmod{p}$	$[x_1, x_3] = x_3^p$	x_2
6	$a_{55}(1 + a_{11}) \equiv 0 \pmod{p}$	$[x_1, x_5] = x_1^p$	x_1
7	$a_{23}(1 + a_{11}) \equiv 0 \pmod{p}$	$[x_1, x_2] = x_1^p$	x_3
8	$a_{21} + a_{21}a_{55} \equiv 0 \pmod{p}$	$[x_2, x_5] = x_4^p$	x_1
9	$a_{31} + a_{31}a_{55} \equiv 0 \pmod{p}$	$[x_3, x_5] = x_4^p$	x_1
10	$a_{35} + a_{11}a_{35} - a_{15}a_{31} - a_{31} \equiv 0 \pmod{p}$	$[x_1, x_3] = x_3^p$	x_1
11	$a_{11}(1 + a_{33}) \equiv 0 \pmod{p}$	$[x_1, x_3] = x_3^p$	x_3
12	$a_{33}(1 + a_{22}) \equiv 0 \pmod{p}$	$[x_2, x_3] = x_2^p$	x_2
13	$a_{55} + a_{33} + a_{33}a_{55} - a_{44} \equiv 0 \pmod{p}$	$[x_3, x_5] = x_4^p$	x_4
14	$a_{55} + a_{22} + a_{22}a_{55} + a_{23}(1 + a_{55}) - a_{44} \equiv 0 \pmod{p}$	$[x_2, x_5] = x_4^p$	x_4
15	$(a_{22} + a_{25})(1 + a_{11}) - a_{15}a_{21} \equiv 0 \pmod{p}$	$[x_1, x_2] = x_1^p$	x_1
16	$a_{35}(1 + a_{23} + a_{22}) - a_{25}(1 + a_{33}) - a_{24} \equiv 0 \pmod{p}$	$[x_2, x_3] = x_2^p$	x_4
17	$-a_{15} - a_{15}a_{22} - a_{15}a_{23} \equiv 0 \pmod{p}$	$[x_1, x_2] = x_1^p$	x_4
18	$-a_{15} - a_{15}a_{33} - a_{34} \equiv 0 \pmod{p}$	$[x_1, x_3] = x_3^p$	x_4

TABLE 1. Table for the group G_1

Now we are ready to prove Theorem B stated in the introduction. In the following proof, by (k) we mean the equation in the k th row of Table 1.

Proof of Theorem B. It follows from Lemma 4.2 that G_1 is of order p^9 , $\Phi(G_1) < Z(G_1)$ and $\gamma_2(G_1) = \Phi(G_1)$ is elementary abelian. It is easy to show that the order of $\text{Autcent}(G_1)$ is p^{20} . Since $\text{Aut}(G_1)$ is elementary abelian for $p = 2$, assume that p is odd. We now prove that

all automorphisms of G_1 are central. Let α be the automorphism of G_1 defined in (4.2), i.e., $\alpha(x_i) = x_i \prod_{j=1}^5 x_i^{a_{ij}}$, where a_{ij} are non-negative integers for $1 \leq i, j \leq 5$. Since $G_1/Z(G_1)$ is elementary abelian, it is sufficient to prove that $a_{ij} \equiv 0 \pmod p$ for $1 \leq i, j \leq 5$.

Since $\alpha(x_1^p) = x_1^{p(1+a_{11})} \prod_{j=2}^5 x_j^{pa_{1j}} \neq 1$, $x_5^p = 1$ and $a_{1j} \equiv 0 \pmod p$ for $2 \leq j \leq 4$, it follows that $1 + a_{11}$ is not divisible by p . Therefore (6) and (7) give $a_{55} \equiv 0 \pmod p$ and $a_{23} \equiv 0 \pmod p$ respectively. Thus by (8) and (9) respectively, we get $a_{21} \equiv 0 \pmod p$ and $a_{31} \equiv 0 \pmod p$. Using the fact that $a_{31} \equiv 0 \pmod p$, (10) reduces to the equation $a_{35}(1 + a_{11}) \equiv 0 \pmod p$. Since $1 + a_{11}$ is not divisible by p , we get $a_{35} \equiv 0 \pmod p$. Observe that $1 + a_{33}$ is not divisible by p . For, suppose p divides $1 + a_{33}$. Since a_{31}, a_{32}, a_{35} divisible by p and $x_4 \in Z(G_1)$, it follows that $\alpha(x_3) \in Z(G_1)$, which is not true. Using this fact, it follows from (11) that $a_{11} \equiv 0 \pmod p$. Using above information, (13), (14) and (15) reduces, respectively, to the following equations.

$$(4.4) \quad a_{33} - a_{44} \equiv 0 \pmod p,$$

$$(4.5) \quad a_{22} - a_{44} \equiv 0 \pmod p,$$

$$(4.6) \quad a_{22} + a_{25} \equiv 0 \pmod p.$$

Subtracting equation (4.5) from equation (4.4), we get $a_{33} - a_{22} \equiv 0 \pmod p$. Adding this to equation (4.6) gives $a_{33} + a_{25} \equiv 0 \pmod p$. Using this fact after adding (12) to equation (4.6), we get $a_{22}(1 + a_{33}) \equiv 0 \pmod p$. Since $1 + a_{33}$ is not divisible by p , $a_{22} \equiv 0 \pmod p$. Thus equations (4.5) and (4.6) give $a_{44} \equiv 0 \pmod p$ and $a_{25} \equiv 0 \pmod p$ respectively. So $a_{33} \equiv 0 \pmod p$ from equation 4.4. Now (16) and (17) give $a_{24} \equiv 0 \pmod p$ and $a_{15} \equiv 0 \pmod p$ respectively. Finally, from equation (18) we get $a_{34} \equiv 0 \pmod p$. Hence all a_{ij} 's are divisible by p , which shows that α is a central automorphism of G_1 . Since α was an arbitrary automorphism of G_1 , we get $\text{Aut}(G_1) = \text{Autcent}(G_1)$.

It now remains to prove that $\text{Aut}(G_1)$ is elementary abelian. Notice that G_1 is purely non-abelian. Since $\gamma_2(G_1) = \Phi(G_1)$, the exponent of $G_1/\gamma_2(G_1)$ is p . That $\text{Aut}(G_1) = \text{Autcent}(G_1)$ is elementary abelian now follows from Theorem 2.1. This completes the proof of the theorem. \square

Finally we proceed to construct a finite p -group G such that $\text{Aut}(G)$ is elementary abelian, $\gamma_2(G) < \Phi(G)$ and $\Phi(G) = Z(G)$ is elementary abelian. Let p be any prime, even or odd. Define the group

$$(4.7) \quad G_2 = \langle x_1, x_2, x_3, x_4 \mid x_1^{p^2} = x_2^{p^2} = x_3^{p^2} = x_4^{p^2} = 1, [x_1, x_2] = 1, \\ [x_1, x_3] = x_4^p, [x_1, x_4] = x_4^p, [x_2, x_3] = x_1^p, [x_2, x_4] = x_2^p, [x_3, x_4] = x_4^p \rangle.$$

It is easy to prove the following lemma.

Lemma 4.4. *The group G_2 is a p -group of order p^8 , $\gamma_2(G_2) < \Phi(G_2)$ and $Z(G_2) = \Phi(G_2)$ is elementary abelian, where p is any prime. Moreover, if p is odd, then G_2 is regular.*

Again, as mentioned in the introduction, it can be checked by using GAP that for $p = 2$, $\text{Aut}(G_2)$ is elementary abelian. So from now onwards, we assume that p is odd. For $1 \leq i \leq 4$, let $e_{x_i} = x_1^{a_{i1}} x_2^{a_{i2}} x_3^{a_{i3}} x_4^{a_{i4}}$, where a_{ij} are non-negative integers for $1 \leq i, j \leq 4$. Let α be an arbitrary automorphism of G_2 . Since the nilpotency class of G_2 is 2 and $\gamma_2(G_2)$ is generated by the set

$\{x_1^p, x_2^p, x_4^p\}$, we can write

$$(4.8) \quad \alpha(x_i) = x_i \prod_{j=1}^4 x_j^{a_{ij}}$$

for some non-negative integers a_{ij} for $1 \leq i, j \leq 4$.

The following table, which will be used in the proof of Theorem C below, is produced in a similar fashion as Table 1.

No.	equations	relations	x_i 's
1	$a_{13} \equiv 0 \pmod p$	$[x_2, x_3] = x_1^p$	x_3
2	$a_{23} \equiv 0 \pmod p$	$[x_2, x_4] = x_2^p$	x_3
3	$a_{43} \equiv 0 \pmod p$	$[x_1, x_3] = x_4^p$	x_3
4	$a_{41} \equiv 0 \pmod p$	$[x_1, x_4] = x_4^p$	x_1
5	$a_{21} \equiv 0 \pmod p$	$[x_2, x_4] = x_2^p$	x_1
6	$a_{24} \equiv 0 \pmod p$	$[x_2, x_4] = x_2^p$	x_4
7	$a_{14} \equiv 0 \pmod p$	$[x_2, x_3] = x_1^p$	x_4
8	$a_{44}(1 + a_{22}) \equiv 0 \pmod p$	$[x_2, x_4] = x_2^p$	x_2
9	$a_{11} + a_{11}a_{44} \equiv 0 \pmod p$	$[x_1, x_4] = x_4^p$	x_4
10	$a_{22} + a_{22}a_{33} + a_{33} - a_{11} \equiv 0 \pmod p$	$[x_2, x_3] = x_1^p$	x_1
11	$-a_{42}(1 + a_{33}) \equiv 0 \pmod p$	$[x_3, x_4] = x_4^p$	x_1
12	$a_{12} + a_{12}a_{44} - a_{42} \equiv 0 \pmod p$	$[x_1, x_4] = x_4^p$	x_2
13	$a_{32} + a_{32}a_{44} - a_{34}a_{42} - a_{42} \equiv 0 \pmod p$	$[x_3, x_4] = x_4^p$	x_2
14	$a_{34}(1 + a_{22}) - a_{12} \equiv 0 \pmod p$	$[x_2, x_3] = x_1^p$	x_2
15	$a_{11}(1 + a_{33} + a_{34}) + a_{33} + a_{34} - a_{44} \equiv 0 \pmod p$	$[x_1, x_3] = x_4^p$	x_4
16	$a_{31} + a_{31}a_{44} + a_{33} + a_{33}a_{44} \equiv 0 \pmod p$	$[x_3, x_4] = x_4^p$	x_4

TABLE 2. Table for the group G_2

Now we are ready to prove Theorem C stated in the introduction. By (k), in the following proof, we mean the equation in the k th row of Table 2.

Proof of Theorem C. It follows from Lemma 4.4 that G_2 is of order p^8 , $\gamma_2(G_2) < \Phi(G_2)$ and $Z(G_2) = \Phi(G_2)$ is elementary abelian. It is again easy to show that the order of $\text{Autcent}(G_2)$ is p^{16} . Since $\text{Aut}(G_2)$ is elementary abelian for $p = 2$, assume that p is odd. As in the proof of Theorem B, to show that all automorphisms of G_2 are central, it is sufficient to show that $a_{ij} \equiv 0 \pmod p$ for $1 \leq i, j \leq 4$.

Since a_{21}, a_{23}, a_{24} are divisible by p , it follows that $(1 + a_{22})$ is not divisible by p . For, if p divides $(1 + a_{22})$, then $\alpha(x_2) \in Z(G_2)$, which is not possible. Using this fact, (8) gives $a_{44} \equiv 0 \pmod p$. Thus from (9) we get $a_{11} \equiv 0 \pmod p$. Now we observe from (10) that $(1 + a_{33})$ is not divisible by p . For, suppose, $(1 + a_{33})$ is divisible by p , then using the fact that $a_{11} \equiv 0 \pmod p$, (10) gives $a_{33} \equiv 0 \pmod p$, which is not possible. Thus (11) gives $a_{42} \equiv 0 \pmod p$. Now using that a_{42} and a_{44} are divisible by p , (12) and (13) give $a_{12} \equiv 0 \pmod p$ and $a_{32} \equiv 0 \pmod p$ respectively. Since $a_{12} \equiv 0 \pmod p$ and $(1 + a_{22})$ is not divisible by p , (14) gives $a_{34} \equiv 0 \pmod p$. Using that a_{11} , a_{34} and a_{44} are divisible by p , (15) gives $a_{33} \equiv 0 \pmod p$. Now using that a_{33} and a_{44} are divisible by p , equation (16) gives $a_{31} \equiv 0 \pmod p$. Since a_{11} and a_{33} are divisible by p , equation (10) gives $a_{22} \equiv 0 \pmod p$. Hence $a_{ij} \equiv 0 \pmod p$ for $1 \leq i, j \leq 4$.

Since $Z(G_2)$ is elementary abelian, $\text{Aut}(G_2) = \text{Autcent}(G_2)$ is elementary abelian by Theorem 2.1. This completes the proof of the theorem. \square

Acknowledgements. Authors thank Prof. Mike Newman for his useful comments and suggestions.

REFERENCES

- [1] J. E. Adney, T. Yen, *Automorphisms of a p -group*, Illinois J. Math. **9** (1965), 137 - 143.
- [2] G. Ban, S. Yu, *Minimal abelian groups that are not automorphism groups*, Arch. Math. (Basel) **70** (1998), 427 - 434.
- [3] Y. Berkovich, Z. Janko, *Groups of prime power order - Volume 2*, Walter de Gruyter, Berlin, New York (2008).
- [4] M. J. Curran, *Semidirect product groups with abelian automorphism groups*, J. Austral. Math. Soc. Ser. A **42** (1987), 84 - 91.
- [5] B. E. Earnley, *On finite groups whose group of automorphisms is abelian*, Ph. D. thesis, Wayne State University (1975), Dissertation Abstracts, V. 36, p. 2269 B.
- [6] *The GAP Group, GAP - Groups, Algorithms, and Programming*, Version 4.4.12, 2008 (<http://www.gap-system.org>).
- [7] P. Hegarty, *Minimal abelian automorphism groups of finite groups*, Rend. Sem. Mat. Univ. Padova **94** (1995), 121 - 135.
- [8] H. Heineken, H. Liebeck, *The occurrence of finite groups in the automorphism group of nilpotent groups of class 2*, Arch. Math. (Basel) **25** (1974), 8 - 16.
- [9] H. Heineken, *Nilpotente Gruppen, deren sämtliche Normalteiler charakteristisch sind*, Arch. Math. (Basel) **33** (1979/80), 497 - 503.
- [10] H. Hilton, *An introduction to the theory of groups of finite order*, Oxford, Clarendon Press (1908).
- [11] C. Hopkins, *Non-abelian groups whose groups of isomorphisms are abelian*, The Annals of Mathematics, 2nd Ser., **29**, No. 1/4. (1927 - 1928), 508-520.
- [12] M. H. Jafari, *Elementary abelian p -groups as central automorphism groups*, Comm. Algebra **34** (2006), 601 - 607.
- [13] V. K. Jain, M. K. Yadav, *On finite p -groups whose automorphisms are all central*, Israel J. Math. **189** (2012), 225 - 236.
- [14] A. Jamali, *Some new non-abelian 2-groups with abelian automorphism groups*, J. Group Theory, **5** (2002), 53 - 57.
- [15] D. Jonah, M. Konvisser, *Some non-abelian p -groups with abelian automorphism groups*, Arch. Math. (Basel) **26** (1975), 131 - 133.
- [16] A. Mahalanobis, *The Diffie-Hellman Key Exchange Protocol and non-abelian nilpotent groups*, Israel J. Math., **165** (2008), 161 - 187.
- [17] G. A. Miller, *A non-abelian group whose group of isomorphism is abelian*, Mess. of Math. **43** (1913-1914), 124 - 125.
- [18] M. Morigi, *On p -groups with abelian automorphism group*, Rend. Sem. Mat. Univ. Padova **92** (1994), 47 - 58.
- [19] M. Morigi, *On the minimal number of generators of finite non-abelian p -groups having an abelian automorphism group*, Comm. Algebra **23** (1995), 2045 - 2065.
- [20] R. R. Struik, *Some non-abelian 2-groups with abelian automorphism groups*, Arch. Math. (Basel) **39** (1982), 299 - 302.

DEPARTMENT OF MATHEMATICS, CENTRAL UNIVERSITY OF BIHAR, PATNA 800 014, INDIA.
E-mail address: jaijinedra@gmail.com

SCHOOL OF MATHEMATICS, HARISH-CHANDRA RESEARCH INSTITUTE, CHHATNAG ROAD, JHUNSI, ALLAHABAD 211019, INDIA.
E-mail address: pradeeprai@hri.res.in

SCHOOL OF MATHEMATICS, HARISH-CHANDRA RESEARCH INSTITUTE, CHHATNAG ROAD, JHUNSI, ALLAHABAD 211019, INDIA.
E-mail address: myadav@hri.res.in